Evaluation Warning: The document was created with Spire.Doc for Python.

**Mate（ 4.1.7版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | Mate |
| 版本 | 4.1.7 |
| 包名 | afcfht.bfeiea.dgcecb |
| 域名线索 | 67条 |
| URL线索 | 88条 |
| APP图标 |  |
| 分析日期 | 2024年11月26日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | mate(1).apk |
| 文件大小 | 64.91MB |
| MD5值 | f58bd7a3e982b6ec55830b7483799259 |
| SHA1值 | 987f6a3f2195617903ef116a1d536c19fc556e5e |
| SHA256值 | 3252496b15cb27802e78b35875302648888dce1bea2450fc2f59b7971dd0252a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Mate |
| 包名 | afcfht.bfeiea.dgcecb |
| 主活动Activity | com.wind.im.MainActivity |
| 安卓版本名称 | 4.1.7 |
| 安卓版本 | 20230710 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| play.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apiinit.amap.com | IP: 203.119.169.174 所属国家: China 地区: Beijing 城市: Beijing  |
| android.bugly.qq.com | IP: 109.244.244.35 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| dualstack-arestapi.amap.com | IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| rqd.uu.qq.com | IP: 109.244.173.225 所属国家: China 地区: Beijing 城市: Beijing  |
| api.weixin.qq.com | IP: 109.244.145.152 所属国家: China 地区: Beijing 城市: Beijing  |
| lbs.amap.com | IP: 59.82.60.56 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| debugx5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| wb.amap.com | IP: 59.82.31.149 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.cn | IP: 49.4.41.160 所属国家: China 地区: Beijing 城市: Beijing  |
| debugtbs.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| api.xmpush.xiaomi.com | IP: 183.84.7.230 所属国家: China 地区: Beijing 城市: Beijing  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| open.weixin.qq.com | IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: California 城市: El Segundo  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| resolver.msg.xiaomi.net | IP: 120.92.96.13 所属国家: China 地区: Beijing 城市: Beijing  |
| playready.directtaps.net | IP: 40.70.71.156 所属国家: United States of America 地区: Virginia 城市: Boydton  |
| login.imgcache.qq.com | IP: 182.254.59.164 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| cfg.imtt.qq.com | IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing  |
| graph.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| norma-external-collect.meizu.com | IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mdc.html5.qq.com | IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 121.36.119.243 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| mst01.is.autonavi.com | IP: 59.82.31.100 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | 没有服务器地理信息.  |
| soft.tbs.imtt.qq.com | IP: 119.167.201.75 所属国家: China 地区: Shandong 城市: Qingdao  |
| store.hispace.hicloud.com | IP: 118.194.33.169 所属国家: China 地区: Shanghai 城市: Shanghai  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| cgi.qplus.com | 没有服务器地理信息.  |
| restsdk.amap.com | IP: 203.119.169.174 所属国家: China 地区: Beijing 城市: Beijing  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| resolver.msg.global.xiaomi.net | IP: 8.219.182.3 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| long.open.weixin.qq.com | IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing  |
| adiu.amap.com | IP: 59.82.29.155 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wap.amap.com | IP: 106.8.157.248 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| 67.211.78.206 | IP: 67.211.78.206 所属国家: Hong Kong 地区: Hong Kong 城市: Cheung Shue Tau  |
| fr.register.xmpush.global.xiaomi.com | IP: 52.29.132.42 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| cgicol.amap.com | IP: 59.82.60.56 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing  |
| openmobile.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| wup.imtt.qq.com | IP: 42.187.184.221 所属国家: China 地区: Beijing 城市: Beijing  |
| mpsapi.amap.com | IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cgi.connect.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| appsupport.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| astat.bugly.qcloud.com | IP: 150.109.27.253 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| pms.mb.qq.com | IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing  |
| idmb.register.xmpush.global.xiaomi.com | IP: 13.127.176.4 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| api-push.meizu.com | IP: 125.94.213.129 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| aexception.bugly.qq.com | IP: 101.226.233.161 所属国家: China 地区: Shanghai 城市: Shanghai  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| www.openssl.org | IP: 23.34.36.190 所属国家: Japan 地区: Osaka 城市: Osaka  |
| log.tbs.qq.com | IP: 109.244.244.32 所属国家: China 地区: Beijing 城市: Beijing  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Beijing 城市: Beijing  |
| material.io | IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/s/h.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/s/h.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/s/h.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/s/h.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/s/h.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/h.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/s/h.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/s/bj.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/s/bj.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/s/bk.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/s/cr.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/s/bf.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://restsdk.amap.com  | com/amap/api/mapcore/util/fe.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/mapcore/util/eq.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/i.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/mapcore/util/gv.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/mapcore/util/ex.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/mapcore/util/b.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/ct.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/cf.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| https://material.io/design/components/dialogs.html  | com/afollestad/materialdialogs/MaterialDialog.java  |
| http://xml.apache.org/xslt  | com/wind/imlib/utils/KitReleaseLogUtils.java  |
| http://%s:%s  | com/wind/imlib/connect/http/HttpConnection.java  |
| http://%s:%s  | com/wind/imlib/connect/http/interceptor/HostInterceptor.java  |
| http://%s:%s  | com/wind/imlib/bean/ServerBucket.java  |
| http://%s:%s/api/exclude/siteConfig/servers  | com/wind/imlib/bean/ServerBucket.java  |
| http://www.baidu.com:3501  | com/wind/im/BuildConfig.java  |
| https://67.211.78.206:7788/  | com/wind/im/BuildConfig.java  |
| http://www.baidu.com:3501  | com/wind/im/WindApp.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gn.java  |
| https://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cw.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gu.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gc.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fq.java  |
| https://api.xmpush.xiaomi.com/v1/trace/report/sdk  | com/xiaomi/push/df.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/o.java  |
| https://resolver.msg.global.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bp.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bp.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/bb.java  |
| http://restsdk.amap.com  | com/loc/s.java  |
| http://restsdk.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/loc/a.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/ff.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/loc/l.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/loc/l.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/loc/fa.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/loc/fa.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/loc/cr.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/ey.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fk.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://restsdk.amap.com/rest/lbs/dem/dataservice?z=%d&x=%d&y=%d&type=2  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://%s:%s  | com/imacapp/home/ui/activity/KitCustomWebViewActivity.java  |
| https://graph.qq.com/  | com/imacapp/wind/api/LoginService.java  |
| https://api.weixin.qq.com/  | com/imacapp/wind/api/LoginService.java  |
| http://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/crashreport/CrashReport.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/a.java  |
| http://aexception.bugly.qq.com:8012/rqd/async  | com/tencent/bugly/crashreport/common/strategy/a.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| http://wup.imtt.qq.com:8080  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/j.java  |
| http://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/a/c.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/b/a/a.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/b/a/a.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://login.imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://login.imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://login.imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/g.java  |
| https://cgi.qplus.com/report/report  | com/tencent/open/utils/l.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/a/d.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| https://play.google.com/store  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com/app/  | Mogua Engine V1  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| http://www.openssl.org/support/faq.html  | lib/x86/libijkffmpeg.so  |
| http://mpsapi.amap.com/ws/mps/vmap  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/rtt  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/smap  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://m5.amap.com  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| ftp@example.com  | lib/x86/libcf-msc.so  |
| o@netstream.failed  | lib/x86/librtmp-jni.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86/libijkplayer.so  |
| v@ro.product  | lib/x86/libAMapSDK\_MAP\_v8\_0\_0.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=cn, ST=ehedam, L=aeccel, O=ciedik, OU=ebbejj, CN=gefcei 签名算法: rsassa\_pkcs1v15 有效期自: 2023-07-06 04:55:36+00:00 有效期至: 2123-06-12 04:55:36+00:00 发行人: C=cn, ST=ehedam, L=aeccel, O=ciedik, OU=ebbejj, CN=gefcei 序列号: 0x3b30afec 哈希算法: sha256 md5值: 5fa38112a7a6bd695bf7d3c0ac673552 sha1值: e6a0325371e59a080a4e885d388e8bf75d94e8cd sha256值: dfc75f7fdef13a5aac57e45a5f091734ff7b7907d35cc149611c2733096a2f60 sha512值: 8c10c71f4bf87d2d500077d5fc2a084a376ae59db1ebc2c39944ddc6c7fb430d569066aea98dbd54d73711153bde320c92d41646f40bbb33afb3af3405397a14**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "wx\_appsecret" : "."  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.BROADCAST\_PACKAGE\_ADDED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_CHANGED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_INSTALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_PACKAGE\_REPLACED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| afcfht.bfeiea.dgcecb.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| afcfht.bfeiea.dgcecb.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| afcfht.bfeiea.dgcecb.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| afcfht.bfeiea.dgcecb.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| afcfht.bfeiea.dgcecb.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.wind.im.MainActivity | **Schemes**: true://,  |
| com.imacapp.common.WindCommTransitActivity | **Schemes**: jmfcim://,  |
| com.tencent.tauth.AuthActivity | **Schemes**: .://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**